UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA

MARGARET JOHNSON and STANA SHESTO, *individually and on behalf of others similarly situated*,	)	
Plaintiffs,	)	**CASE NO. 2:20-cv-42**
v.	)	**CLASS ACTION**
THE METHODIST HOSPITALS, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs, Margaret Johnson and Stana Shesto, individually, and on behalf of all others similarly situated, bring this action against Defendant, The Methodist Hospitals, Inc. ("TMH" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff, Margaret Johnson, is and at all times mentioned herein was, an individual citizen of the State of Indiana residing in the City of Kingsford Heights.

2. Plaintiff, Stana Shesto, is and at all times mentioned herein was, an individual citizen of the State of Indiana residing in the City of Crown Point.

3. Defendant TMH is an Indiana healthcare organization with its principal place of business in Gary, Indiana.

4. This Court has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because Plaintiffs assert claims that necessarily raise substantial disputed federal issues under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Federal Trade Commission Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801). Jurisdiction is proper in this Court because the principal place of business for the Defendant is in Gary, Indiana, and because the conduct at issue in this case occurred in Indiana. Venue is proper in this Court because a substantial portion of the acts and transactions that constitute violations of law complained of herein occurred in this venue.

NATURE OF THE ACTION

5. This class action arises out of the recent cyberattack and data breach ("Data Breach") at TMH's medical facilities. As a result of the Data Breach, Plaintiffs and approximately 68,000 class members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs' and class members' sensitive personal information—which was entrusted to TMH, its officials and agents—was compromised and unlawfully accessed due to the Data Breach. Information compromised in the Data Breach includes names, demographic information, dates of birth, Social Security numbers, driver's license or identification card numbers, employment information, health insurance information, medical information, other protected health information as defined by HIPAA, and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant TMH collected and maintained (collectively the "Private Information").

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of class members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and

other Class members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant TMH's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, TMH and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had TMH properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant TMH collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names, but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiffs and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and class members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) intrusion upon seclusion, (iii) negligence *per se*, (iv) breach of express contract, (v) breach of implied contract, and (vi) breach of fiduciary duty.

DEFENDANT'S BUSINESS

16. Defendant TMH is in the business of rendering healthcare services, medical care, and treatment.

17. Defendant offers a full spectrum of healthcare services and has on staff more than 400 physicians and 2,500 employees.

18. In the ordinary course of receiving treatment and health care services from Defendant TMH, patients are required to provide Defendant with sensitive, personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information, and;
- Other information that may be deemed necessary to provide care.

19. Defendant TMH also gathers certain medical information about patients and creates records of the care it provides to them.

20. Additionally, Defendant TMH may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care", such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

21. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, TMH promises to, among other things, : A) provide

patients with "[p]ersonal privacy", and B) maintain the "[c]onfidentiality of [patients'] clinical records."[1]

22. In addition, TMH promises that it "is committed to providing quality health care and respecting the privacy and confidentiality of your medical information," and further promises that "[ou]r policies and procedures regarding access to and release of medical records conform to state and federal laws and are designed to safeguard your privacy."[2]

THE CYBERATTACK AND DATA BREACH

23. In June 2019, TMH was struck by a targeted and sophisticated cyberattack.

24. According to news reports, two Methodist employees fell victim to an email phishing scheme that allowed an unauthorized actor to gain access to the employees' email accounts.

25. According to an investigation conducted by Defendant, one email account was subject to unauthorized access from March 13 to June 12, 2019 and another account was subject to unauthorized access between June and July of 2019.

26. TMH had no processes in place to discover that its computer systems had been compromised by this cyberattack, and was unaware of the cyberattack for an extended period of time.

27. Even though the unauthorized activity began as early as March 2019, TMH claims it did not learn of the breach until several months later in August of 2019.

28. The compromised email accounts contained messages and email attachments that included PHI of at least 68,000 patients.

---

[1] *See* https://www.methodisthospitals.org/patients/patient-rights/.

[2] https://www.methodisthospitals.org/about_methodist/epic/mychart/

29. The types of data exposed included names, addresses, email addresses, telephone numbers, dates of service, treatment information, health insurance information, Social Security numbers, treating and referring physicians' names, and medical bill account numbers.

30. Plaintiffs believe their Private Information was stolen (and subsequently sold) in the Data Breach. In fact, Defendant admitted it could not rule out the possibility of unauthorized data access and data exfiltration in the course of its forensic investigation.[3]

31. Despite this, TMH did not notify affected patients until October of 2019.

32. Defendant had obligations created by federal law, including HIPAA, contract, industry standards, common law, and representations made to Plaintiffs and class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiffs and class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

34. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

35. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller

---

[3] https://www.databreaches.net/in-methodist-hospitals-notifies-68039-after-two-employees-fall-for-phishing-attack/

municipalities and ***hospitals*** are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[4]

36. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant TMH.

37. Defendant breached its obligations to Plaintiffs and class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the TMH computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

---

[4] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (emphasis added).

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

38. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the

cyberattack, Defendant TMH negligently and unlawfully failed to safeguard Plaintiffs' and class members' Private Information.

39. Accordingly, as outlined below, Plaintiffs' and class members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

40. Cyberattacks and data breaches at medical facilities like TMH are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

41. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

42. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyberattacks and related data breaches.

43. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[5]

44. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[6]

---

[5] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks

[6] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

45. Similarly, cyberattacks and related data security incidents inconvenience patients. The various inconveniences patients encounter as a result of such incidents include, but are not limited:

a. rescheduling medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. losing patient medical history.[7]

46. Cyberattacks are considered a breach of HIPAA Rules because unauthorized access to PHI is prohibited under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40[8]

47. Data breaches represent yet another problem for patients who have already experienced inconvenience and disruption associated with a cyberattack.

48. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

---

[7] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/; https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech

[8] *Id.*

[9] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

49. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

50. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

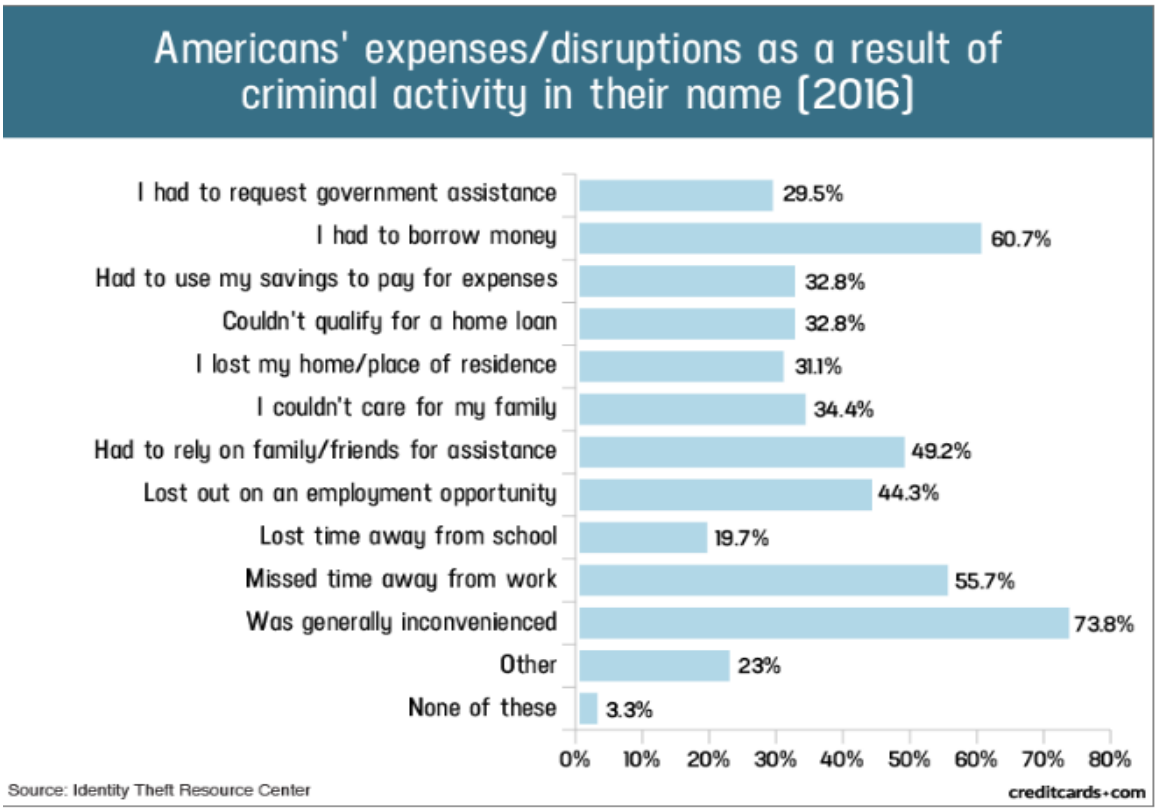
51. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[11]

---

[10] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

[11] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at:

https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).



52. PII/PHI is a valuable property right.[12] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value.

53. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance

[12] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

and payment records, and credit report may be affected."[13] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

54. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

55. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

56. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and class members must vigilantly monitor their financial and medical accounts for many years to come.

---

[13] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2014).

57. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[14]

58. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

59. To date, Defendant has done nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach including, but not limited to, the costs and loss of time they incurred because of the disruption of service at Defendant' medical facilities.

60. Plaintiffs and Class members have been damaged by the compromise of their Private Information in the Data Breach.

61. Plaintiff Margaret Johnson's medical records, PII, and PHI were compromised as a direct and proximate result of the Data Breach.

62. Plaintiff Stana Shesto's medical records, PII, and PHI were compromised as a direct and proximate result of the Data Breach. Following the Data Breach, Ms. Shesto was forced to sign up for Credit Karma and now continually spends time monitoring her credit report for

[14] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

unauthorized activity. She also spent time researching the impact the Data Breach might have on her Private Information.

63. As a direct and proximate result of Defendant' conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

64. As a direct and proximate result of Defendant' conduct, Plaintiffs and Class members have been forced to expend time dealing with the effects of the Data Breach.

65. Plaintiffs and Class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

66. Plaintiffs and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and class members.

67. Plaintiffs and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

68. Plaintiffs and Class members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

69. Class members were also damaged via benefit-of-the-bargain damages. Such class members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant TMH's computer property and Plaintiffs' and Class

members' Private Information. Thus, Plaintiffs and the Class members did not get what they paid for.

70. Plaintiffs and Class members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

71. Plaintiffs and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. In addition to the loss of use of and access to their medical records and costs associated with the inability to access their medical records (including actual disruption of medical care and treatment), many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding alternative medical care and treatment;

b. Delaying or foregoing medical care and treatment;

c. Undergoing medical care and treatment without medical providers having access to a complete medical history and records;

d. Having to retrace or recreate their medical history;

e. Finding fraudulent charges;

f. Canceling and reissuing credit and debit cards;

g. Purchasing credit monitoring and identity theft prevention;

h. Addressing their inability to withdraw funds linked to compromised accounts;

i. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

j. Placing "freezes" and "alerts" with credit reporting agencies;

k. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

l. Contacting financial institutions and closing or modifying financial accounts;

m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

72. Moreover, Plaintiffs and Class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

73. Further, as a result of Defendant' conduct, Plaintiffs and Class members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of their right.

74. As a direct and proximate result of Defendant' actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

75. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

76. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons who utilized Defendant TMH's services and whose Private Information was maintained on Defendant TMH's system that was compromised in the Data Breach.

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

77. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, the class consists of approximately 68,000 patients of Defendant TMH whose data was compromised in Data Breach.

78. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to class members to safeguard their Private Information;

f. Whether Defendant breached its duty to class members to safeguard their Private Information;

g. Whether computer hackers obtained class members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

79. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class member, was compromised in the Data Breach.

80. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

81. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and class members, in that all the Plaintiffs' and class members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

82. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

83. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

FIRST COUNT

Negligence
(On Behalf of Plaintiffs and All Class Members)

84. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 83 above as if fully set forth herein.

85. Defendant required Plaintiffs and Class members to submit non-public personal information in order to obtain medical services.

86. By collecting and storing this data in its computer property, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

87. Defendant owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

88. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach.

89. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

90. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

91. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

92. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to class members' Private Information;

e. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

f. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

93. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

94. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to class members.

95. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach

96. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

SECOND COUNT

Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

97. Plaintiffs repeats and re-alleges each and every allegation contained in Paragraphs 1 through 83 as if fully set forth herein.

98. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

99. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class members' seclusion under common law.

100. By intentionally failing to keep Plaintiffs' and Class members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class members' private affairs in a manner that identifies Plaintiffs and Class members and that would be highly offensive and objectionable to an ordinary person; and

b. Intentionally publicizing private facts about Plaintiffs and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class members.

101. Defendant knew that an ordinary person in Plaintiffs' or Class members' position would consider Defendant's intentional actions highly offensive and objectionable.

102. Defendant invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

103. Defendant intentionally concealed from Plaintiffs and Class members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

104. The conduct described above was at or directed at Plaintiffs and the Class Members.

105. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant' conduct amounted to a substantial and serious invasion of Plaintiffs' and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

106. In failing to protect Plaintiffs' and Class members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class members' rights to have such information kept confidential and private. Plaintiffs, therefore, seeks an award of damages on behalf of themselves and the Class.

THIRD COUNT

Breach of Express Contract
(On Behalf of Plaintiffs and All Class Members)

107. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 83 above as if fully set forth herein.

108. Plaintiffs and members of the Class allege that they entered into valid and enforceable express contracts, or were third party beneficiaries of valid and enforceable express contracts, with Defendant.

109. The valid and enforceable express contracts that Plaintiffs and Class members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

110. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and members of the Class agreed to pay money for these services.

111. Both the provision of healthcare and the protection of Plaintiffs' and Class members' PII/PHI were material aspects of these contracts.

112. At all relevant times, Defendant expressly promised to, among other things, A) provide patients with "[p]ersonal privacy", and B) maintain the "[c]onfidentiality of [patients'] clinical records."[15]

113. On information and belief, Defendant also promised to maintain the privacy and confidentiality of Plaintiffs' Private information in its applicable privacy policy.

114. Defendant's express representations formed an express contract requiring Defendant's to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' PII/PHI.

115. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiffs and Class members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class members would not have entered into these contracts with Defendant and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

116. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PII/PHI to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

117. Plaintiffs and Class members performed their obligations under the contract.

118. Defendant materially breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

---

[15] *See* https://www.methodisthospitals.org/patients/patient-rights/.

119. Defendant did not maintain the privacy of Plaintiffs' and Class members' PII/PHI as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 68,000 Class members. Specifically, Defendant did not comply with industry standards, or otherwise protect Plaintiffs' and the Class members' PII/PHI, as set forth above.

120. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

121. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

122. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class members, nor any reasonable person would have obtained healthcare from Defendant and/or its affiliated healthcare providers.

123. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

124. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

FOURTH COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

125. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 83 above as if fully set forth herein.

126. When Plaintiffs and Class members provided their Private Information to Defendant TMH in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

127. Defendant solicited and invited class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

128. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

129. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

130. Plaintiffs and Class members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

131. Plaintiffs and Class members fully and adequately performed their obligations under the implied contracts with Defendant.

132. Defendant breached its implied contracts with Class members by failing to safeguard and protect their Private Information.

133. As a direct and proximate result of Defendant's breaches of the implied contracts, Class members sustained damages as alleged herein.

134. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

135. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

FIFTH COUNT

Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

136. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 83 above as if fully set forth herein.

137. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

138. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

139. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is

a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

140. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information.

141. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act, HIPAA, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

142. Defendant's failure to comply with applicable federal laws and regulations constitutes negligence *per se*.

143. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

144. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

145. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

SIXTH COUNT

Breach of Fiduciary Duty
(On Behalf of Plaintiffs and All Class Members)

146. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 83 above as if fully set forth herein.

147. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

148. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

149. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

150. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

151. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

152. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

153. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

154. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

155. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

156. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

157. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

158. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

159. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

160. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

161. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

162. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

163. As a direct and proximate result of Defendant' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual disruption of ongoing medical care and treatment; (ii) actual identity theft; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant' possession and is subject to further unauthorized disclosures so long as Defendant

fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vii) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (viii) the diminished value of Defendant' services they received.

164. As a direct and proximate result of Defendant' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of reasonable punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demands a jury trial on all issues so triable.

Dated: January 30, 2020

Respectfully submitted,

/s/ *Gary M. Klinger, Esq.*

KOZONIS & KLINGER, LTD.
Gary M. Klinger
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60630
Phone: 312.283.3814
Fax: 773.496.8617
gklinger@kozonislaw.com

WHITFIELD BRYSON & MASON LLP
Gary E. Mason (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
Fax: 202.429.2294
gmason@wbmllp.com

Attorneys for Plaintiffs and the Proposed Class